Deutscher Bundestag **Drucksache 17/6989**

17. Wahlperiode 12. 09. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Agnes Malczak, Omid Nouripour, Tom Koenigs, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 17/6825 –

Cyber-Strategie der Bundesregierung – Militärische und verteidigungspolitische Aspekte

Vorbemerkung der Fragesteller

Die „Cyber-Sicherheitsstrategie für Deutschland" der Bundesregierung vom Februar 2011 betrachtet den Schutz des Cyber-Raums als existentielle Frage des 21. Jahrhunderts. Um Sicherheit im Cyber-Raum zu gewährleisten, strebt sie eine enge internationale Zusammenarbeit an und hebt hierbei insbesondere die NATO hervor. Nach Behördenangaben und Meinung von Expertinnen und Experten hat die Bedrohung des Cyber-Raums in jüngster Zeit zugenommen und mit neuen, insbesondere staatlichen Akteuren eine neue Qualität erreicht. Als eine Antwort darauf wurde am 16. Juni 2011 das Nationale Cyber-Abwehrzentrum vom Bundesministerium des Innern eröffnet, mit dem künftig schneller auf Angriffe reagiert und das Krisenmanagement optimiert werden soll.

Es gibt berechtigte Zweifel, ob die Strategie der Bundesregierung und das neue Cyber-Abwehrzentrum geeignet sind, die Sicherheit des Cyber-Raums in Deutschland zu verbessern. Es fehlt an technischer Expertise und Ressourcen, um komplexe und gefährliche Angriffe überhaupt zu erkennen und darauf zu reagieren. Auch die militärischen und verteidigungspolitischen Aspekte von Internetsicherheit in Deutschland bleiben diffus. Dabei basieren laut Cyber-Strategie der Bundesregierung die hochtechnisierten Formen des Krieges im Informationszeitalter „auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischer Fähigkeiten".

In Bezug auf die Gefährdungslage und Cyber-Sicherheit in der Bundeswehr fragen wir daher die Bundesregierung:

Vorbemerkung der Bundesregierung

Hinsichtlich der nachrichtendienstlichen Aspekte der Anfrage ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die erbetene Auskunft geheimhaltungsbedürftig ist. Die Anfrage zielt auf Einzelheiten tatsächlicher oder vermuteter nachrichtendienstlicher Aktivitäten, die

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Verteidigung vom 8. September 2011 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

grundsätzlich nicht öffentlich dargestellt werden können. Aus ihrer Offenlegung könnten sowohl staatliche Akteure anderer Länder als auch nichtstaatliche Akteure Rückschlüsse auf die Fähigkeiten und Methoden des Bundesnachrichtendienstes ziehen. Im Ergebnis würde dadurch die Funktionsfähigkeit unserer Sicherheitsbehörden und damit die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

Gleichwohl ist die Bundesregierung selbstverständlich bereit, dem Informationsrecht des Parlamentes unter Wahrung berechtigter Geheimhaltungsinteressen nachzukommen. Deshalb hat die Bundesregierung die erbetenen Informationen als „VS-Vertraulich“ eingestufte Verschlusssache an die Geheimschutzstelle des Deutschen Bundestages zur Einsicht durch entsprechend berechtigte Personen gemäß den Geheimschutzvorschriften übermittelt.

1. Welche über das Krisenmanagement und die Fähigkeit zur Angriffserkennung und Schadensbekämpfung hinausreichende Aktivitäten im Bereich Cyber-Sicherheit gibt es innerhalb der Bundeswehr?

Aus militärischer Sicht umfasst Cyber-Sicherheit (Cybersecurity) sowohl die Gewährleistung der Nutzbarkeit des Cyber-Raums wie auch die Nutzung des Cyber-Raums zur Förderung sicherheitspolitischer Interessen. Maßnahmen der IT-Sicherheit gehören hierzu ebenso wie die IT-Betriebsführung, die Ausbildung von Fähigkeiten zum Wirken im und durch den Cyber-Raum und die verteidigungspolitische Förderung von Verhaltensregeln und Transparenz zur Stärkung internationaler Sicherheit und Stabilität.

2. Inwiefern führt die Bundeswehr Angriffssimulationen im Cyber-Raum durch?

Angriffssimulationen im oder über den technischen Informationsraum (Internet) finden nicht statt. Im Rahmen ihrer Ausbildung führen die Computer-Netzwerk-Operations-Kräfte (CNO-Kräfte) der Bundeswehr Übungen in der eigenen Ausbildungs- und Trainingseinrichtung durch. Hierbei handelt es sich jedoch um eine abgeschlossene Laborumgebung ohne Verbindung zum Internet.

3. Inwiefern führt die Bundeswehr auch über die eigenen Systeme hinausreichende Aufklärungsaktivitäten durch?

Die Bundeswehr führt im Rahmen der Nationalen Krisenvorsorge generell Aufklärung in allen Dimensionen militärischer Handlungsmöglichkeiten durch.

4. Welche Forschungsaktivitäten gibt es?

Die Bundeswehr arbeitet mit der deutschen IT-Sicherheitsindustrie sowie zivilen und militärischen Forschungseinrichtungen zur schritthaltenden Entwicklung von Strategien und Schutzmechnanismen zum Schutz der eigenen IT-Netzwerke gegen Angriffe aus dem Cyber-Raum zusammen.

Darüber hinaus nutzen alle mit dem technischen Informationsraum befassten Kräfte der Bundeswehr die öffentlich zugänglichen Erkenntnisse von Forschungsaktivitäten in aller Welt und unterhalten zu ihrer auftragsbezogenen Aus- und Weiterbildung Kontakte mit den jeweiligen Expertiseträgern.

5. Inwiefern führt die Bundeswehr auch Maßnahmen zum Aufbau offensiver Fähigkeiten durch?

Die Bundeswehr erwirbt Fähigkeiten, um im Rahmen ihres verfassungsgemäßen Auftrages auch im Cyber-Raum wirken zu können.

6. Welche über das Krisenmanagement und die Fähigkeit zur Angriffserkennung und Schadensbekämpfung hinausreichende Aktivitäten im Bereich Cyber-Sicherheit gibt es innerhalb des Bundesnachrichtendienstes?

7. Inwiefern führt der Bundesnachrichtendienst Angriffssimulationen im Cyber-Raum durch?

8. Inwiefern führt der Bundesnachrichtendienst auch über die eigenen Systeme hinausreichende Aufklärungsaktivitäten durch?

9. Gibt es Forschungsaktivitäten, und wenn ja, welche?

10. Gibt es Maßnahmen zum Aufbau offensiver Fähigkeiten, und wenn ja, welche?

Bezüglich der Antworten zu den Fragen 6 bis 10 wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. Inwiefern bedient sich die Bundeswehr im Rahmen von Auslandseinsätzen besonderer Cyber-Fähigkeiten, für deren Vorhaltung bzw. Anwendung ein Mandat des Deutschen Bundestages erforderlich ist?

Auf die Antwort zu Frage 12 wird verwiesen.

12. Inwieweit wurde in der Vergangenheit bei Auslandseinsätzen der Bundeswehr bereits auf Fähigkeiten der Bundeswehr im Bereich des elektronischen Kampfes im bzw. aus dem Cyber-Raum zurückgegriffen?

Bisher wurden die CNO-Kräfte der Bundeswehr nicht bei Auslandseinsätzen eingesetzt.

13. Inwiefern ist die Abteilung Computer und Netzwerkoperationen (CNO) in der Tomburg-Kaserne in Rheinbach, die dem Kommando Strategische Aufklärung unterstellt ist, die einzige Dienststelle der Bundeswehr, die für den Bereich Cyber-Sicherheit sowie den elektronischen Kampf im Cyber-Raum abgestellt ist?

Zur Rolle der CNO-Kräfte wird auf die Antwort zu Frage 15 verwiesen.

Für die Cyber-Sicherheit im IT-System der Bundeswehr ist die IT-Sicherheitsorganisation der Bundeswehr mit dem Computer Emergency Response Team der Bundeswehr (CERTBw) verantwortlich.

14. Inwiefern berät die Abteilung CNO Stellen der Bundesregierung wie das Bundesamt für Sicherheit in der Informationstechnik, das Bundesministe-

rium des Innern oder aber das neu eingerichtete Nationale Cyber-Abwehrzentrum?

Die Bundeswehr ist im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) im Rahmen von Kooperationsvereinbarungen mit Personen aus den Bereichen IT-AmtBw (IT-Sicherheit/Cyber Defence), Streitkräfteunterstützungskommando (IT-Betrieb) und MAD Amt (IT-Abschirmung) vertreten. Die CNO-Kräfte der Bundeswehr sind im (Cyber-AZ) nicht vertreten. Eine Beratung von Stellen der Bundesregierung über das Bundesministerium der Verteidigung (BMVg) hinaus durch Kräfte der Abteilung CNO im Kommando Strategische Aufklärung findet nicht statt.

15. Welchen konkreten Auftrag hat die Abteilung CNO, und welche rechtliche Grundlage gibt es für ihre Arbeit?

CNO-Kräfte sind dazu aufgestellt, im Rahmen des verfassungsgemäßen Auftrages der Bundeswehr Fähigkeiten zum Wirken im Cyber-Raum bereitzustellen.

16. Welche Kooperationen der Bundeswehr mit den Streitkräften anderer Staaten existieren im Bereich Cyber-Security, und welcher Natur sind diese Kooperationen im Einzelnen?

Das BMVg hat ein bilaterales Abkommen (Memorandum of Understanding) mit den Streitkräften der Vereinigten Staaten von Amerika (United States European Command USEUCOM) abgeschlossen. Im Rahmen dieser Vereinbarung werden Informationen zu Schwachstellen in IT-Systemen und Softwareprodukten sowie zu aktuellen IT-Sicherheitsvorfällen ausgetauscht.

Im Rahmen der trinationalen Zusammenarbeit zwischen Deutschland, Österreich und der Schweiz wurde eine Arbeitsgruppe Cyber Defence eingerichtet, die derzeit die Möglichkeiten des Informationsaustausches und der Zusammenarbeit zum Schutz der militärischen IT-Netzwerke gegen Angriffe aus dem Cyber-Raum untersucht.

17. Welche Ergebnisse zeitigte die jeweilige bilaterale Zusammenarbeit in Bezug auf Cyber-Security mit den USA, Frankreich, Großbritannien und der Schweiz?

Im Rahmen der bilateralen Zusammenarbeit mit den USA werden kontinuierlich technische Informationen zur Cyber-Sicherheit ausgetauscht, die zur eigenen Beurteilung der Cyber-Sicherheitslage beitragen.

Deutschland unterstützt die Schweiz beim Aufbau einer Partnerschaft mit dem NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estland.

Eine bilaterale Zusammenarbeit mit Großbritannien und Frankreich zur Cyber-Sicherheit findet derzeit mit der Bundeswehr nicht statt.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

18. Was sind Inhalt und bisherige Ergebnisse des seit November 2010 stattfindenden Dialogs mit den USA (Cyber Command beim US-Militär und Fort Meade bei der National Security Agency)?

Die militärpolitischen Gespräche zur Cyber-Sicherheit zwischen dem BMVg und dem US-amerikanischen Verteidigungsministerium, die seit November 2010 geführt werden, dienen der gegenseitigen Information über verteidigungspolitische Bewertungen, Maßnahmen und Ziele der jeweiligen Cyber-Politik.

Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

19. Was sind Inhalt und bisherige Ergebnisse des Erfahrungsaustausches unter Regierungsressorts mit der Schweiz im Bereich Cyber-Sicherheit?

Gegenstand des gemeinsam mit dem Bundesministerium des Innern durchgeführten Erfahrungsaustauschs mit schweizer Regierungsvertretern ist die Entwicklung einer nationalen Cyber-Sicherheitsstrategie, der Aufbau von IT-Sicherheitsstrukturen sowie die Diskussion von Möglichkeiten der Entwicklung eines Kodex für Staatenverhalten im Cyber-Raum im Rahmen von OSZE und VN.

20. Welche Organisationen stehen für die Bundeswehr bei der internationalen Kooperation im Bereich Cyber-Sicherheit im Mittelpunkt?

Aus verteidigungspolitischer Sicht kommt insbesondere der NATO als Fundament der transatlantischen Sicherheit im Bereich der Cyber-Sicherheit eine besondere Bedeutung zu, wie dies auch im 2010 beschlossenen Strategischen Konzept der NATO Ausdruck findet. Die bereits im Juni 2011 beschlossene NATO Cyber Defence Policy belegt die besondere Relevanz, die Fragen der Cyber-Sicherheit von den Mitgliedstaaten der NATO zugemessen wird.

Insbesondere im Kontext vertrauens- und sicherheitsbildender Maßnahmen sowie der Vereinbarung eines internationalen Kodex für Staatenverhalten im Cyber-Raum spielen auch die OSZE und die Vereinten Nationen eine besondere Rolle.

21. Welche Anstrengungen zur internationalen Kooperation unternimmt die Bundeswehr mit welchen Ergebnissen im Rahmen der EU, insbesondere der Gemeinsamen Sicherheits- und Verteidigungspolitik?

In der Europäischen Union befassen sich sowohl die EU-Kommission als auch der Europäische Auswärtige Dienst und die European Network and Information Security Agency (ENISA) auf verschiedenen Ebenen mit Fragen der Cyber-Sicherheit. Dabei ist die enge Abstimmung mit der NATO von besonderer Bedeutung, da sich beide Organisationen sinnvoll ergänzen können. Die Bundeswehr unterstützt diesen Prozess im Rahmen der ständigen engen Zusammenarbeit bzw. unmittelbar durch die in EU bzw. NATO entsandten Mitarbeiterinnen und Mitarbeiter.

22. Welche Implikationen hat die Beschreibung des Cyber-Raums im Cyber-Bericht der Bundeswehr als 5. Operationsdimension für die Mandatspflicht von Cyber-Operationen seitens der Bundeswehr?

Die Zustimmung des Deutschen Bundestages ist nach § 1 Absatz 2 des Parlamentsbeteiligungsgesetzes bei jedem Einsatz bewaffneter deutscher Streitkräfte

außerhalb des Geltungsbereichs des Grundgesetzes erforderlich. Ausgehend von den in der Cyber-Sicherheitsstrategie für Deutschland beschriebenen Maßnahmen zur Abwehr von Cyber-Angriffen sieht die Bundesregierung keinen Anwendungsfall des Parlamentsbeteiligungsgesetzes.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333